H. Kawasaki
9/8/03
Q77157
1 of 1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　９月１０日

出願番号
Application Number: 特願２００２－２６４０７２

[ST. 10/C]: [ＪＰ２００２－２６４０７２]

出願人
Applicant(s): 日本電気株式会社

２００３年　７月２８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５９６４７

【書類名】　特許願
【整理番号】　53210759
【提出日】　平成14年 9月10日
【あて先】　特許庁長官　殿
【国際特許分類】　H04B 7/26
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　川崎　晴夫
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100088328
【弁理士】
【氏名又は名称】　金田　暢之
【電話番号】　03-3585-1882
【選任した代理人】
【識別番号】　100106297
【弁理士】
【氏名又は名称】　伊藤　克博
【選任した代理人】
【識別番号】　100106138
【弁理士】
【氏名又は名称】　石橋　政幸
【手数料の表示】
【予納台帳番号】　089681
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9710078

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　端末ロックシステムおよび端末ロック方法

【特許請求の範囲】

【請求項１】　利用者が正当な権利を有する者であることを確認する本人確認を行うことにより、第三者による端末装置の不正使用を防止するための端末ロックシステムであって、

近距離無線通信を行うための無線通信手段を備え、携帯可能なキー側装置と、

近距離無線通信を行うことによりキー側装置への接続要求を行い、接続が確認できたキー側装置の情報と予め登録されている情報とが一致しなかった場合、またはキー側装置との間で近距離無線通信による接続が確認できない場合、装着されている端末装置の使用を禁止する端末側装置と、

から構成されている端末ロックシステム。

【請求項２】　前記キー側装置には、予め前記端末側装置の情報が登録されていて、接続を要求してきた端末側装置の情報と予め登録されている情報とが一致した場合のみ近距離無線通信による接続を行う請求項１記載の端末ロックシステム。

【請求項３】　前記キー側装置は、特定の操作が行われた場合にのみ近距離無線通信を開始する請求項１または２記載の端末ロックシステム。

【請求項４】　利用者が正当な権利を有する者であることを確認する本人確認を行うことにより、第三者による端末装置の不正使用を防止するための端末ロック方法であって、

近距離無線通信を行うための無線通信手段を備えるとともに携帯可能なキー側装置の情報を、端末装置に設けられた端末側装置に登録するステップと、

前記端末側装置が、近距離無線通信を行うことによりキー側装置への接続要求を行うステップと、

接続が確認できたキー側装置の情報と予め登録されている情報とが一致しなかった場合、またはキー側装置との間で近距離無線通信による接続が確認できない場合、前記端末側装置が装着されている端末装置の使用を禁止するステップと、

から構成されている端末ロックシステム。

【請求項５】　前記キー側装置は、接続を要求してきた端末側装置の情報と予め登録されている情報とが一致した場合のみ近距離無線通信による接続を行うステップをさらに備えた請求項４記載の端末ロック方法。

【請求項６】　前記キー側装置は、特定の操作が行われた場合にのみ近距離無線通信を開始する請求項４または５記載の端末ロック方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、利用者が正当な権利を有する者であることを確認する本人確認を行うことにより、第三者による端末装置の不正使用を防止するための端末ロックシステムおよび方法に関する。

【０００２】

【従来の技術】

近年、パソコンやＰＤＡ、携帯電話機等の端末装置が普及し、多くのユーザがこのような端末装置を利用するようになっている。しかし、このような端末装置には重要な個人情報が記憶されている場合があり、他人による不正使用を防止することが要求される。

【０００３】

端末の不正使用を防止するための個人認証の仕組みは従来から存在する。まず、パスワードを毎回入力させることで本人を特定する方法があるが、この方法では利用者にとっては不便であり、パスワードの管理等の問題も発生し、操作も煩雑である。

【０００４】

また、ＩＤカードを利用して認証を行ったり、利用時に１回だけ有効となるワンタイムパスワードを自動的に発行するというパスワード入力の応用例もあるが、端末装置から離れる時にはＩＤカード等を端末装置から取り出し、端末装置を使用する場合にはＩＤカード等を端末装置に挿入する等の操作が必要となるため操作が煩雑となる。また、端末装置から離れる際にＩＤカード等を取り出すのを忘れたのでは第三者が容易に不正使用を行うことができてしまう。また、携帯電

話機等に適用した場合、着信を待つ間は携帯電話機等を動作状態にする必要があるため常にＩＤカード等を挿入状態とすることが予想される。そのため、携帯電話機等をＩＤカード等ごと紛失した場合には、第三者の不正使用を防止することができない。

【０００５】

さらに、虹彩や声紋、指紋等を使用するバイオ認証技術を用いて個人認証を行う技術もある。しかし、これらの技術は現在のところ、機器のコストが高く、各種の端末装置において認証を行うためだけに導入するには費用がかかるため現実的ではない。

【０００６】

上述した以外の不正使用を防止する従来技術としては、例えば特許文献１（「不正使用防止機能を有する無線通信機」）に記載されたシステムが存在する。このシステムは、無線通信機等を紛失したり盗難等にあった場合、この無線通信機に遠隔地から不正使用を禁止するための指示を与えることにより、無線通信機として動作しないようにするものである。しかし、この従来技術では、無線指示によって使用禁止の動作を行っているため、無線通信機の電源がオンになっている状態で、かつ無線が届く範囲になければ、使用禁止の指示を送信できない。また、この従来技術では、使用禁止にするための操作が必要となるので、席をはずす間にパソコンを使用できなくするような用途に利用したのでは、パスワードを入力させて本人確認をするよりも操作が煩雑となり現実的ではない。

【０００７】

【特許文献１】

特開平０８－１６２９９４号公報

【０００８】

【発明が解決しようとする課題】

上述した従来技術では、第三者による端末装置の不正使用を防止するためには利用者に煩雑な操作を要求することになり、また利用者がパスワードの漏洩、ＩＤカード等ごと紛失したというような場合には第三者の不正使用を確実に防止することはできないという問題点があった。

【０００９】

本発明の目的は、利用者に煩雑な操作を要求することなく本人確認を行い、第三者による端末装置の不正使用を確実に防止することができる端末ロックシステムおよび端末ロック方法を提供することである。

【００１０】

【課題を解決するための手段】

上記目的を達成するために、本発明の端末ロックシステムは、利用者が正当な権利を有する者であることを確認する本人確認を行うことにより、第三者による端末装置の不正使用を防止するための端末ロックシステムであって、

近距離無線通信を行うための無線通信手段を備え、携帯可能なキー側装置と、

近距離無線通信を行うことによりキー側装置への接続要求を行い、接続が確認できたキー側装置の情報と予め登録されている情報とが一致しなかった場合、またはキー側装置との間で近距離無線通信による接続が確認できない場合、装着されている端末装置の使用を禁止する端末側装置とから構成されている。

【００１１】

本発明によれば、キー側装置を身につけた利用者が端末側装置を装着した端末装置から離れ、端末側装置とキー側装置との間で近距離無線通信による接続ができなくなると、端末側装置は装着されている端末装置の使用を禁止してロック状態とする。そのため、利用者には何の操作を要求することなく本人確認を行い、第三者による端末装置の不正使用を確実に防止することができる。

【００１２】

また、前記キー側装置に、予め前記端末側装置の情報を登録しておき、接続を要求してきた端末側装置の情報と予め登録されている情報とが一致した場合のみ近距離無線通信による接続を行うようにしてもよい。

【００１３】

本発明によれば、キー側装置に情報が予め登録されていない装置がキー側装置に接続要求をしてきた場合には、近距離無線通信を行わないようにすることにより、より信頼性の向上を図ることができる。

【００１４】

さらに、前記キー側装置は、特定の操作が行われた場合にのみ近距離無線通信を開始するようにしてもよい。

【００１５】

本発明によれば、利用者が使用する場合のみ特定の操作を行うことによりキー側装置を未起動状態から無線接続の待ち受け状態となるようにしているので、消費電力を削減し電池寿命を延ばすことができる。

【００１６】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して詳細に説明する。

【００１７】

（第１の実施形態）

図１は本発明の第１の実施形態の端末ロックシステムの構成を示すブロック図である。本実施形態の端末ロックシステムは、ブルートゥース（Ｂｌｕｅｔｏｏｔｈ）や無線ＬＡＮ等の近距離無線通信技術を利用して、簡易に個人認証を行うとともに、所有者以外の人間が勝手に端末装置を利用することを防止するシステムを提供するものである。

【００１８】

本実施形態の端末ロックシステムは、図１に示すように、端末側装置１００と、キー側装置２００とから構成される。端末側装置１００は、保護を行いたいパソコンやＰＤＡ、携帯電話等の情報機器に付加、もしくは組み込んで使用するものである。キー側装置２００は、端末装置の正当な所有者が常に身につけて持ち歩くものであり、例えば、携帯電話やＰＤＡ、腕時計やバッジ、キーホルダー等に付加、もしくは組み込んで使用するものである。ここで例示したように、携帯電話やＰＤＡは、端末側装置１００を実装する機器の対象でもあるし、キー側装置２００を実装する機器の対象でもある。

【００１９】

先ずは、本実施形態の端末ロックシステムの概略の動作について説明する。予め端末側装置１００に、キー側装置２００の情報の登録を行っておく。キー側装置２００は、常に端末側装置１００からの接続を待ち受ける状態にしておく。端

末側装置１００は、電源を入れた後、キー側装置２００に対して、近距離無線通信による接続を試みる。このとき、キー側装置２００が無線通信範囲内にあれば、接続が成功するので、端末側装置１００を利用する権利を得ることができる。つまり、一旦情報の登録を行えば、それ以降は、キー側装置２００が、ブルートゥースや無線ＬＡＮ等の近距離無線の通信範囲内にある場合のみ、端末側装置１００を利用することができる。この結果、キー側装置２００を、常に所有者本人が身につけて持ち歩くことにより、所有者が無線通信範囲内にいない場合は、端末装置を利用不可にすることができる。例えば、所有者が携帯電話を紛失したとしても、キー側装置が無線通信範囲内にない限り、使用できない。また、所有者がいない間に、ノートパソコン等を勝手に使用するといった不正使用を未然に防ぐことができる。

【００２０】

次に、本実施形態の端末ロックシステムの詳細な構成について以下に説明する。図１を参照すると、本実施形態の端末ロックシステムは、端末装置に設けられる端末装置側装置１００と、利用者３００が携帯するキー側装置２００とから構成される。

【００２１】

端末側装置１００は、実際にはパソコンやＰＤＡ、携帯電話等の、所有者以外の人間が使用できないように制限したい端末装置に付加、もしくは組み込んで使用する。同様に、キー側装置２００も、実際には携帯電話やＰＤＡ、腕時計やバッジ、キーホルダー等、所有者が常に身につけるような装置に付加、もしくは組み込んで使用する。ここで例示したように、携帯電話やＰＤＡは、端末側装置１００を実装する機器の対象でもあるし、キー側装置２００を実装する機器の対象でもある。

【００２２】

さらに、端末装置側装置１００は、ブルートゥースや無線ＬＡＮ等の近距離無線通信を行うための無線装置１１０と、プログラム制御により動作するコンピュータ（中央処理装置）１２０と、ユーザインタフェース装置１３０とから構成される。また、キー側装置２００は、ブルートゥースや無線ＬＡＮ等の無線装置２

１０と、プログラム制御により動作するコンピュータ（中央処理装置）２２０とから構成されている。

【００２３】

コンピュータ（中央処理装置）１２０は、通信制御部１２１と、端末側装置制御部１２２と、記憶装置１２３とを含む。同様に、コンピュータ（中央処理装置）２２０は、通信制御部２２１と、キー側装置制御部２２２とを含む。

【００２４】

通信制御部１２１は、無線装置１１０を制御する無線制御機能と、実装する無線技術に適した通信プロトコルを使用して通信を実行する機能とを含む。また、通信制御部１２１は、端末側装置制御部１２２から指示されたキー側装置２００に接続するために、無線装置１１０に対して指示を行い、接続の成功または失敗の通知を端末側装置制御部１２２に返却する。

【００２５】

端末側装置制御部１２２は、端末側装置１００を起動したタイミングで、記憶装置１２３に、キー側装置情報が登録されているかどうかをチェックする。まだキー側装置情報が登録されていない場合は、利用可能な状態を維持し、利用者３００が、ユーザインタフェース装置１３０を介して何らかの指示を行うまで待機する。逆に、記憶装置１２３に、キー側端末装置情報が登録されている場合は、まず端末装置全体を利用不可状態にロックする。その後、登録情報に従い、キー側装置２００に対して接続を行うよう、通信制御部１２１に指示を行う。通信制御部１２１から接続の成功が通知された場合は、端末側装置１００を利用可能な状態に遷移させる。通信制御部１２１から接続の失敗が通知された場合は、端末側装置１００を、利用不可状態のまま維持し、使用を禁止する。

【００２６】

また端末側装置制御部１２２はそれ以外に、ユーザインタフェース装置１３０を介して利用者３００からの指示を受け、キー側装置情報の登録、削除、編集等を行う。キー側装置２００の登録を指示された場合、キー側装置２００に対して接続を行うよう、通信制御部１２１に指示を行う。通信制御部１２１から接続の成功が通知された場合は、記憶装置１２３に、キー側装置２００の情報を登録し

て記憶するとともに、ユーザインタフェース装置１３０を介して利用者３００に登録が成功したことを通知する。通信制御部１２１から接続の失敗が通知された場合は、ユーザインタフェース装置１３０を介して利用者３００に登録が失敗したことを通知する。

【００２７】

通信制御部２２１は、無線装置２１０を制御する無線制御機能と、実装する無線技術に適した通信プロトコルを使用して通信を実行する機能とを含む。キー側装置制御部２２２から指示された場合、無線装置２１０に指示して端末側装置１００からの接続を待ち受ける。キー側装置制御部２２２は、通信制御部２２１に対して、端末側装置１００からの接続を待ち受けるよう指示する。

【００２８】

次に、図１及び図２、図３のフローチャートを参照して本実施形態の全体の動作について詳細に説明する。

【００２９】

まず、端末側装置１００の動作について図２のフローチャートを参照して説明する。

【００３０】

端末側装置１００が起動されると、端末側装置制御部１２２は、記憶装置１２３を参照し、キー端末情報が登録されているかどうかをチェックする（ステップ１）。最初は情報が登録されていないため、端末側装置１００は、接続されている端末装置を利用可能な状態としたままで、利用者３００からの入力を待つ（ステップ２）。なお、記憶装置１２３は、半永久的に情報を記憶できる、不揮発性の記憶装置であるものとする。もしくは、揮発性記憶装置であっても、起動時に外部記憶装置から情報を読み込むようにすれば使用することができる。

【００３１】

次に、ステップ２において、利用者３００が、ユーザインタフェース装置１３０を介して、端末側装置制御部１２２に対してキー側装置２００の情報を登録するよう指示を行う。この場合、キー側装置２００を特定するために、キー側装置２００だけが持っている固有の情報を、ユーザインタフェース装置１３０から直

接、入力する手段を提供しても良いし、さもなければ、実装する無線技術に従って、機器探索等の機能を使用して、付近にある機器の一覧を作成し、その一覧の中から選択する等の手段を提供しても良い。

【００３２】

端末側装置制御部１２２は、利用者３００からのキー側装置２００を登録する指示を受け、無線装置１１０を通して、適切な無線通信プロトコルでキー側装置２００に対して接続を試みる（ステップ３）。なお、キー側装置２００を特定するための情報は、装置固有の製造番号であったり、アドレスであったり、ソフトウェア的な識別番号であったりする。少なくとも無線通信の範囲内で、相手側装置を一意に特定できる情報であるものとする。

【００３３】

次に、キー側装置２００の動作について図３のフローチャートを参照して説明する。

【００３４】

キー側装置２００は、電源投入と同時に、キー側装置制御部２２２が通信制御部２２１に指示を行い、端末側装置１００からの接続を待ち受ける（ステップ２１）。通信制御部２２１はこれに従い、端末側装置１００から接続が来るまで待機している。

【００３５】

この状態で、図２のステップ３により、端末側装置１００の無線装置１１０からの接続を、キー側装置２００の無線装置２１０が受信し、互いの無線通信プロトコルを使って通信制御部１２１と通信制御部２２１は、それぞれ接続するための処理を行う。その後、キー側装置２００では、接続の結果を判定する（ステップ２２）。

【００３６】

接続が成功した場合、そのまま端末側装置１００との接続を維持し続ける（ステップ２３）。このとき、実装している無線通信技術に固有の、省電力の仕組みを利用し、電力消費を最小限に抑えることで、接続を維持した状態を保つものとする。

【００３７】

端末側装置１００との接続が切断された場合、起動直後の状態に戻り（ステップ２４）、キー側装置制御部２２２が通信制御部２２１に指示を行い、端末側装置１００からの接続を待ち受ける（ステップ２１）。また、接続が切断されない間は（ステップ２４）、接続を維持した状態が保たれる（ステップ２３）。

【００３８】

再び、図２に戻り端末側装置１００の動作について説明する。

【００３９】

通信制御部１２１は、ステップ３におけるキー側装置２００との接続成功または接続失敗について、端末側装置制御部１２２に通知する。端末側装置制御部１２２は、接続の成功を受け取った場合（ステップ４）、記憶装置１２３にキー側装置２００の情報を書き込み記憶する（ステップ６）。このとき、書き込む情報は、キー側装置２００を特定するための情報でなければならない。できれば、容易に偽造することができないような何らかの特殊演算を行って、その結果を登録するのが望ましい。

【００４０】

その後、端末側装置制御部１２２は、ユーザインタフェース装置１３０を介して、利用者３００に、指定されたキー側装置２００の登録に成功した旨を通知する（ステップ７）。

【００４１】

ステップ４で、端末側装置制御部１２２が接続の失敗を受け取った場合、ユーザインタフェース装置１３０を介して、利用者３００に、指定されたキー側装置２００の登録に失敗した旨を通知する（ステップ５）。その後、端末側装置１００は利用可能なままの状態で、利用者３００からの入力を待ち、キー側装置２００の登録をやり直せるようにする（ステップ２）。

【００４２】

ところで、図２のステップ１において、すでに記憶装置１２３にキー側装置２００の情報が登録されていた場合、端末側装置制御部１２２は、端末側装置１００を利用不可に設定する（ステップ８）。

【００４３】

端末側装置１００を利用不可にしたままの状態で、端末側装置制御部１２２は、記憶装置１２３に登録してあるキー側装置２００の情報をもとに、無線装置１１０を通して、適切な無線通信プロトコルでキー側装置２００に対して接続を試みる（ステップ９）。なお、キー側装置２００を特定するための情報は、装置固有の製造番号であったり、アドレスであったり、ソフトウェア的な識別番号であったりするが、記憶するときに何らかの特殊演算を行っている場合は、逆演算を行う等して元の情報を特定する。少なくとも無線通信の範囲内で、相手側装置を一意に特定できる情報であるものとする。

【００４４】

通信制御部１２１は、ステップ９におけるキー側装置２００との接続成功または接続失敗について、端末側装置制御部１２２に通知する。端末側装置制御部１２２は、接続の成功を受け取った場合（ステップ１０）、端末側装置を利用可能にする（ステップ１１）。

【００４５】

その後、端末側装置制御部１２２は、ユーザインタフェース装置１３０を介して、利用者３００に、指定されたキー側装置２００との接続に成功し、端末側装置１００が利用可能である旨を通知する。

【００４６】

端末側装置１００と、キー側装置２００との間の無線接続は、維持したままにしておく（ステップ１３）。このとき、通常は、実装している無線通信技術に特有の、省電力の仕組みを利用し、電力消費を最小限に抑えることで、接続を維持した状態を保つ。このようにして、端末側装置１００と、キー側装置２００との間の無線接続が維持されている間だけ、端末を利用できるよう動作を行う。

【００４７】

キー側装置２００との接続が切断された場合（ステップ１４）、端末側装置制御部１２２は、端末側装置１００を利用不可にする（ステップ１５）。ステップ１５の状態になった場合、端末側装置１００の利用を終了して、電源をオフにする準備ができた状態と考えられる。ただし、無線通信が異常切断された場合は、

自動的に復旧を行う等の処置を行うべきであり、通信の復旧が不可能であると判断した場合のみ、利用不可にするものとする。また、接続が切断されない間は（ステップ１４）、接続を維持した状態を保つ（ステップ１３）。

【００４８】

なお、ステップ９において端末側装置制御部１２２が通信制御部１２１から接続の失敗を受け取った場合（ステップ１０）、ユーザインタフェース装置１３０を介して、利用者３００に、指定されたキー側装置２００との接続に失敗し、端末側装置１００が利用不可である旨を通知する（ステップ１６）。当然この場合、端末側装置１００は、利用不可のままである。

【００４９】

本実施形態の端末ロックシステムによれば、登録時に一度、認証作業を行う必要はあるが、一旦、登録してしまえば、それ以降は、認証済みのキー側装置２００を常に身につけているだけで、自動的に認証を行うことができる。そのため、利用者は、自分が認証されていることさえ気づかないまま、端末装置を利用するための認証を実行することができる。これにより、利用者に煩雑な操作を要求することなく、利用者が無意識のうちに個人認証を実行できることができる。

【００５０】

また、本実施形態の端末ロックシステムによれば、認証済みの機器が無線通信の範囲内にある場合のみ、機器の利用を可能にするため、例えば、利用者が携帯電話を紛失してしまった場合にも、キー側装置が通信範囲内にない限り、他者はそれを不正使用することができない。これにより、利用者以外の人間が端末装置を不正使用することを防止できる。また、キー側装置と端末側装置とは、直接接続せずに近距離無線通信により接続されるため、キー側装置と端末側装置を同時に紛失するといった事態が発生することはほとんどあり得ない。そのため、端末装置の紛失という場合でも、第三者による不正使用を確実に防止することができる。

【００５１】

さらに、本実施形態の端末ロックシステムによれば、端末側装置も、キー側装置も、通信手段には依存しないことから、一般に広く普及している近距離無線通

信技術を利用でき、ソフトウェア部分の修正だけで互換性の維持が可能になる。本発明は、ただ単に接続できれば良い、という点に基づいており、異企業間のシステムであっても、同じ種類の無線技術を実装している以上、かなり高い確率で接続できるはずであり、また接続さえできればこのシステムを実現することができるのである。しかも、端末側装置もキー側装置もお互いに、「相手が自分をどのように登録しているか」を知る必要がないため、相互接続性について考慮しなければならない事項が少ない。そのため、異企業間のシステム同士が容易に連携できるのである。

【００５２】

さらに、本実施形態の端末ロックシステムによれば、上述したように、端末側装置も、キー側装置も、通信手段には依存しないことから、一般に広く普及している近距離無線通信技術を利用できるため、すでに他の目的で該当する近距離無線通信技術を実装している機器は、ソフトウェアの追加のみでシステムを実現することができる。また、認証にしか使えない、というシステムではなく、実装している近距離無線通信技術は、当然、他の目的にも使用できるため、利用者にとっては、付加価値があるのである。その結果、システム構成が技術的に平易になり、コストも安価になる。

【００５３】

（第２の実施形態）

次に、本発明の第２の実施形態の端末ロックシステムについて図面を参照して詳細に説明する。図４において、図１中の構成要素と同一の構成要素には同一の符号を付し、説明を省略するものとする。

【００５４】

本実施形態の端末ロックシステムは、端末側装置１００と、キー側装置４００とから構成されている。

【００５５】

本実施形態の端末ロックシステムにおけるキー側装置４００は、図４に示すように、無線装置２１０と、コンピュータ４２０と、ユーザインタフェース装置２３０とから構成されている。コンピュータ４２０は、図１に示したキー側装置２

００におけるコンピュータ２２０に対して、記憶装置２２３が新たに設けられている点が異なっている。

【００５６】

上記第１の実施形態の端末ロックシステムでは、キー側装置２００には何も情報が記憶されておらず、端末側装置１００からの接続を待つだけであった。そのため、意図しない装置から接続される可能性もある。これに対し、図４に示した本実施形態の端末ロックシステムにおけるキー側装置４００のコンピュータ４２０には、記憶装置２２３が含まれている。記憶装置２２３を実装することにより、端末側装置１００と同じように、キー側装置４００も、相手側の機器である端末側装置１００の情報を登録することができる。これにより、意図しない相手からの接続を無視したり、利用者３００に通知したりといった対応が可能になる。例えば、悪意のある第三者がキー側装置の情報を入手しようとして、キー側装置に接続してきたような場合でも、本実施形態の端末ロックシステムによれば、キー側装置の情報を悪意のある第三者に知られることを防ぐことができる。

【００５７】

上記第１および第２の実施形態では、端末側装置１００とキー側装置２００、４００が接続するにあたって、特に条件を設けていないが、言うまでもなく、登録時の接続において、パスワード等を使用し、より強力な信頼関係を構築しても良い。パスワード等の入力は、利用者にとっては煩雑な作業であるが、キー側装置２００、４００の情報登録時に１回、行うだけなので大きな負担にはならない。図４のキー側装置４００にはユーザインタフェース装置１３０が含まれている。これにより、利用者はキー側装置４００にも入力できるようになるため、端末側装置１００およびキー側装置４００との間で、パスワードを交換する等が可能になり、より強力な信頼関係を構築できるようになる。製造番号やアドレス、ソフトウェア的な識別番号等の、機器固有の情報に加えて、パスワードのような、当人しか知り得ない情報を含んで特殊演算を行うことで、登録する情報を生成すれば、他人による、なりすまし等を防止できる確率が高くなる。さらに信頼関係を重視する場合、登録情報を定期的に、あるいは何かのタイミングによって作成し直すような処理を組み込めば、さらに信頼度が増す。端末側装置１００および

キー側装置２００、４００が合意して、接続時にお互いしか知り得ない秘密の情報を受け渡しすることで、信頼性を向上させる方法も考えることができる。当然、無線通信の弱点であるセキュリティを考慮し、暗号化によって他者からガードする構成も考えられる。

【００５８】

さらに、上記第１および第２の実施形態では、端末側装置１００の記憶装置１２３に、キー側装置２００、４００の情報を１件しか登録しないものとして説明したが、これは言うまでもなく説明を簡便にするために制限したに過ぎず本発明はこのような場合に限定されるものではない。端末側装置１００の記憶装置１２３に複数のキー側装置の情報を登録するようにしてもよい。この場合、記憶装置１２３に登録されているキー側装置の情報を何らかの順番、あるいは一度に接続チェックし、登録してある情報のうちのいずれか１つと接続を確立できたら、利用可能と判断するといった対応が可能になる。同様に、上記第２の実施形態のようにキー側装置４００が記憶装置２２３を持つシステム構成の場合には、キー側装置４００の記憶装置２２３に複数の端末側装置の情報を登録するようにしてもよい。

【００５９】

また、上記第１および第２の実施形態では説明していないが、端末側装置１００もしくはキー側装置２００、４００がユーザインタフェース装置１３０、２３０を備えている場合、当然、登録している機器情報に対して、利用者の利便性を向上させるための登録名や登録日付、有効期間等の付加情報を追加することも可能であるし、情報の保護、追加、削除、編集等の操作も可能である。

【００６０】

また、上記第１および第２の実施形態では、端末側装置１００とキー側装置２００、４００が接続している間のみ、該当する端末装置を利用可能である、と説明しているが、これは説明を簡便にするために記述した規則に過ぎない。本発明の意図するところは、この両者の装置が、無線通信の範囲内にあるかどうかに基づく、ということであるから、必ずしも、常時、接続を維持していなければならないことを意味するものではない。例えば、実装している近距離無線通信技術が

持つ、機器探索等の機能を使用して、相手装置が無線通信範囲内にいることが確認できれば良いのである。つまり、認証のために最初の１回のみ接続を行い、接続が成功したら切断し、以後は一定時間ごとに相手装置が無線通信範囲内にいるかどうかを、機器探索等の機能を使用してチェックするようなシステム構成も有り得る。極端に言えば、認証のための、最初の１回の接続さえも省略できる。常に一定時間ごとに相手装置が無線通信範囲内にいるかどうかを機器探索等でチェックするだけで実現することも可能である。これらの方法も、本発明の他の実施形態と言える。

【００６１】

さらに、上記第１および第２の実施形態では、端末側装置１００やキー側装置２００、４００の起動直後、自動的に動作を開始するよう説明しているが、装置の起動時以外のタイミングで動作を開始することも当然、可能である。例えばパソコンのスクリーンセーバー等の制御に応用できる。利用者がパソコンから離れ、無線通信範囲の外に出ると、自動的にスクリーンセーバーを起動してパソコンをロック状態にし、他者が覗き見たり、不正な操作を行ったりといった行為を防止できる。この場合、利用者が無線通信範囲内に戻るとスクリーンセーバーを解除し、利用可能な状態に復帰できる。

【００６２】

また、上記第１および第２の実施形態では、キー側装置２００、４００は常に無線接続を待ち受ける状態となっているものとして説明しているが、消費電力の観点から、この方法が望ましくない場合、普段は未起動状態にしておいて、使用するときにワンタッチで起動する等の簡便な操作で無線接続を待ち受けるような処理にすることも可能である。この場合、すべて自動で処理するような構成に比べると、利用者が認証を意識しなければならない分、不便になるが、キーをワンタッチする程度の代償で、代わりに電池寿命が延びるようであれば十分であると言える。

【００６３】

【発明の効果】

以上説明したように、本発明によれば、利用者に煩雑な操作を要求することな

く本人確認を行い、第三者による端末装置の不正使用を確実に防止することができるという効果を得ることができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態の端末ロックシステムの構成を示すブロック図である。

【図２】

図１の端末側装置１００の動作を示すフローチャートである。

【図３】

図１のキー側装置２００の動作を示すフローチャートである。

【図４】

本発明の第２の実施形態の端末ロックシステムの構成を示すブロック図である。

【符号の説明】

１～１６　　ステップ

２１～２４　　ステップ

１００　　端末側装置

１１０　　無線装置

１２０　　コンピュータ（中央処理装置）

１２１　　通信制御部

１２２　　端末側装置制御部

１２３　　記憶装置

１３０　　ユーザインタフェース装置

２００　　キー側装置

２１０　　無線装置

２２０　　コンピュータ（中央処理装置）

２２１　　通信制御部

２２２　　キー側装置制御部

２３０　　ユーザインタフェース装置

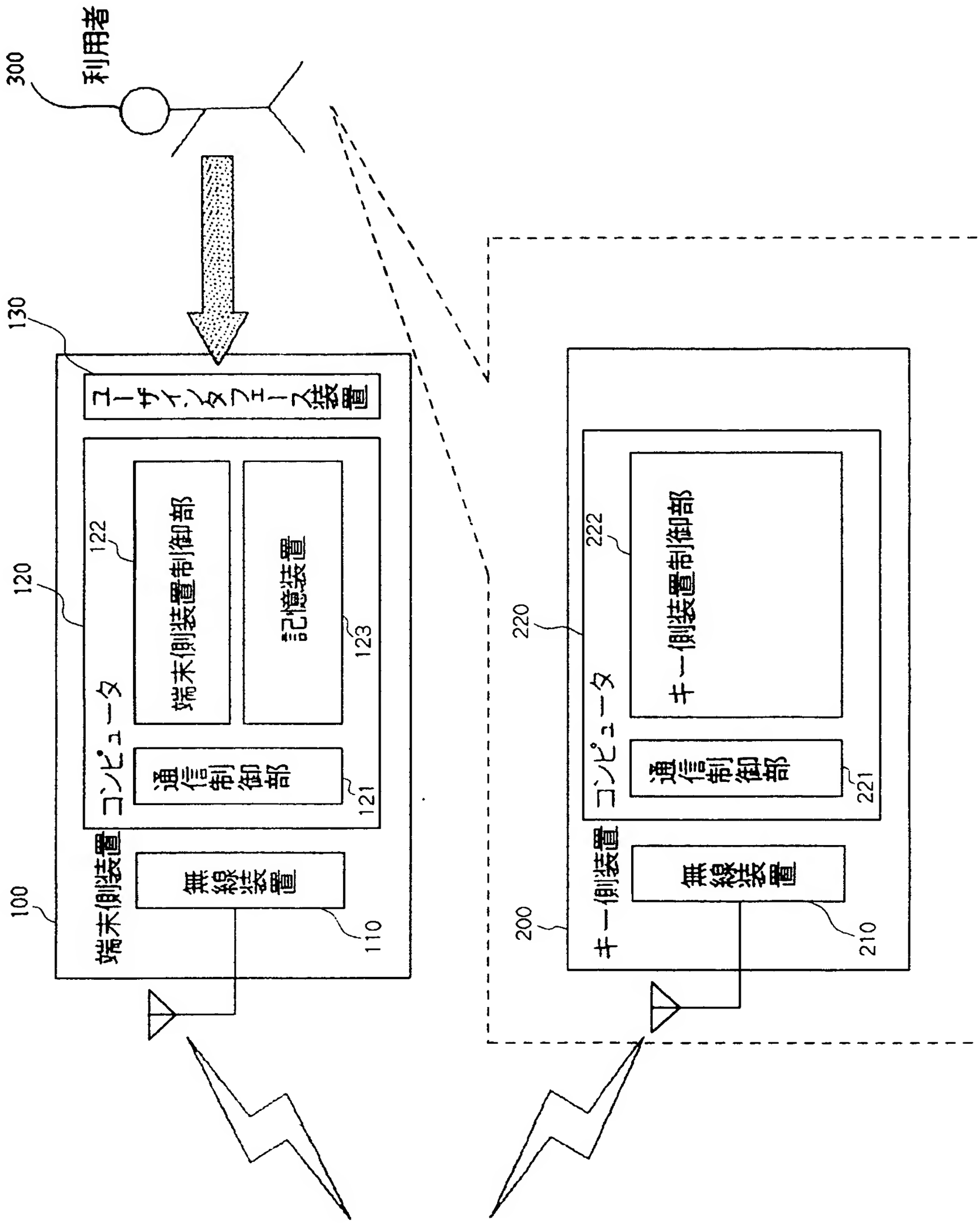
３００　利用者

４００　キー側装置

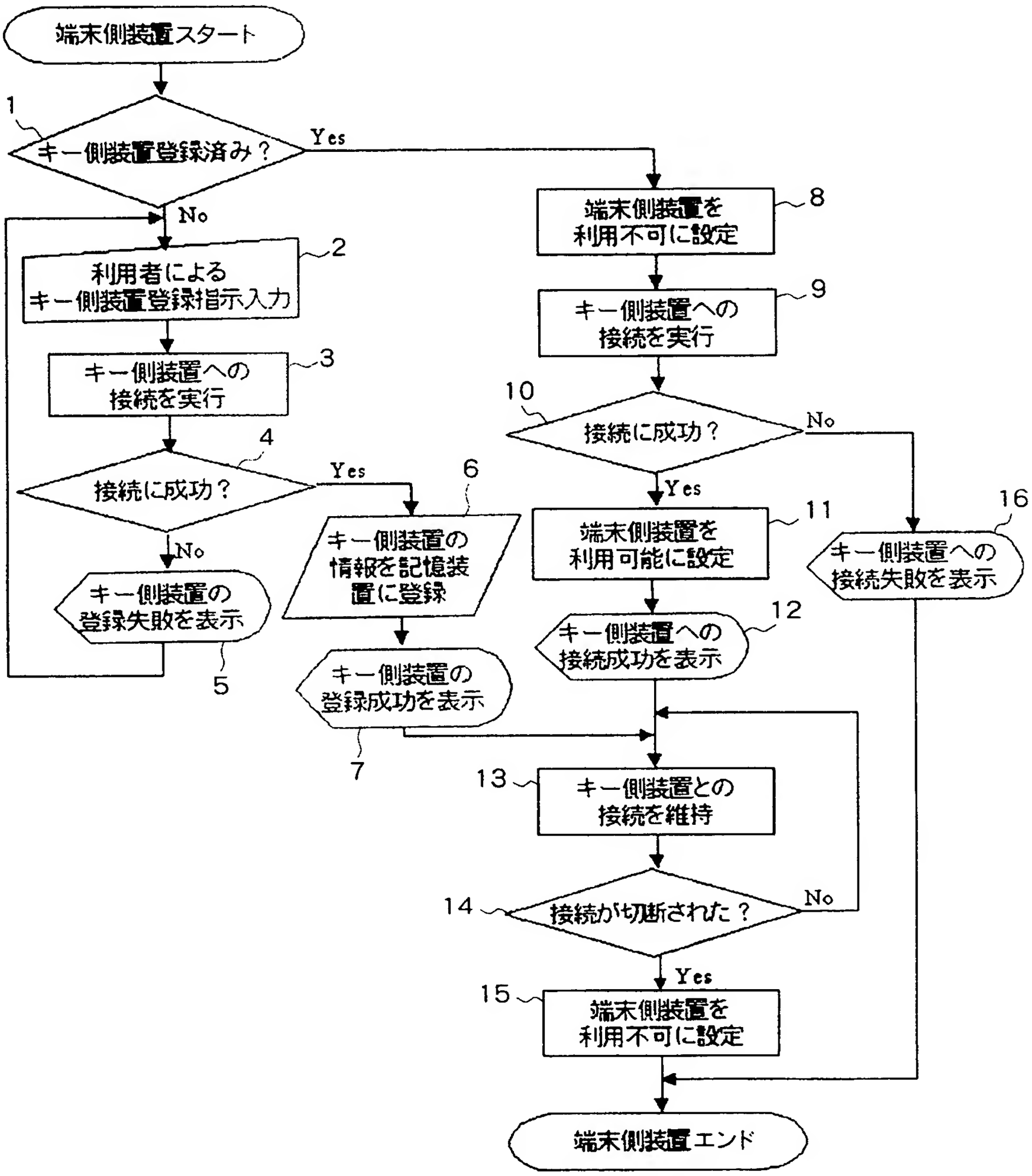
４２０　コンピュータ（中央処理装置）

【書類名】　図面

【図１】

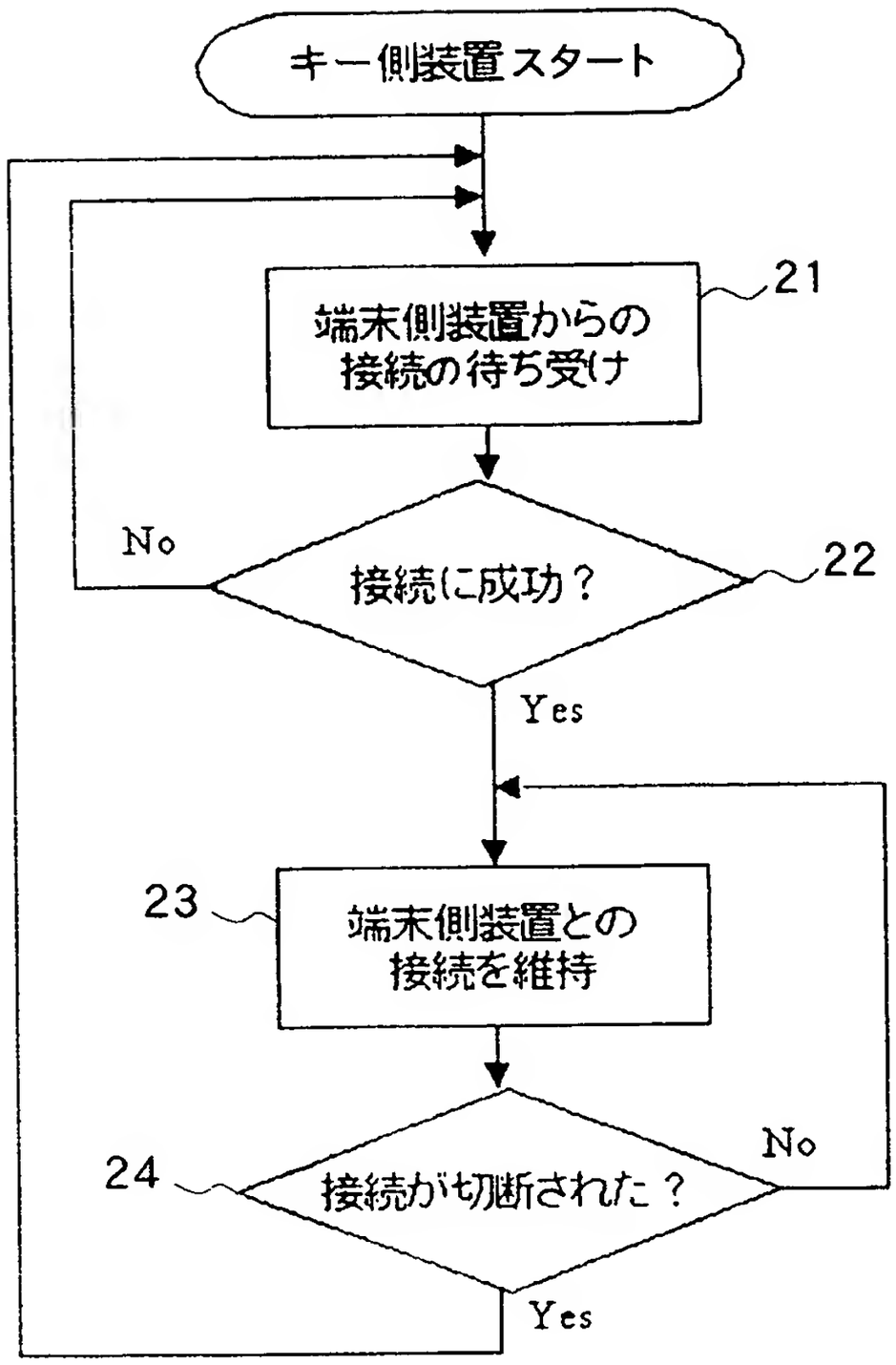

300
利用者
130
ユーザインタフェース装置
120
コンピュータ
122
端末側装置制御部
記憶装置
123
通信制御部
121
端末側装置
無線装置
110
100
220
コンピュータ
222
キー側装置制御部
通信制御部
221
キー側装置
無線装置
210
200

【図２】

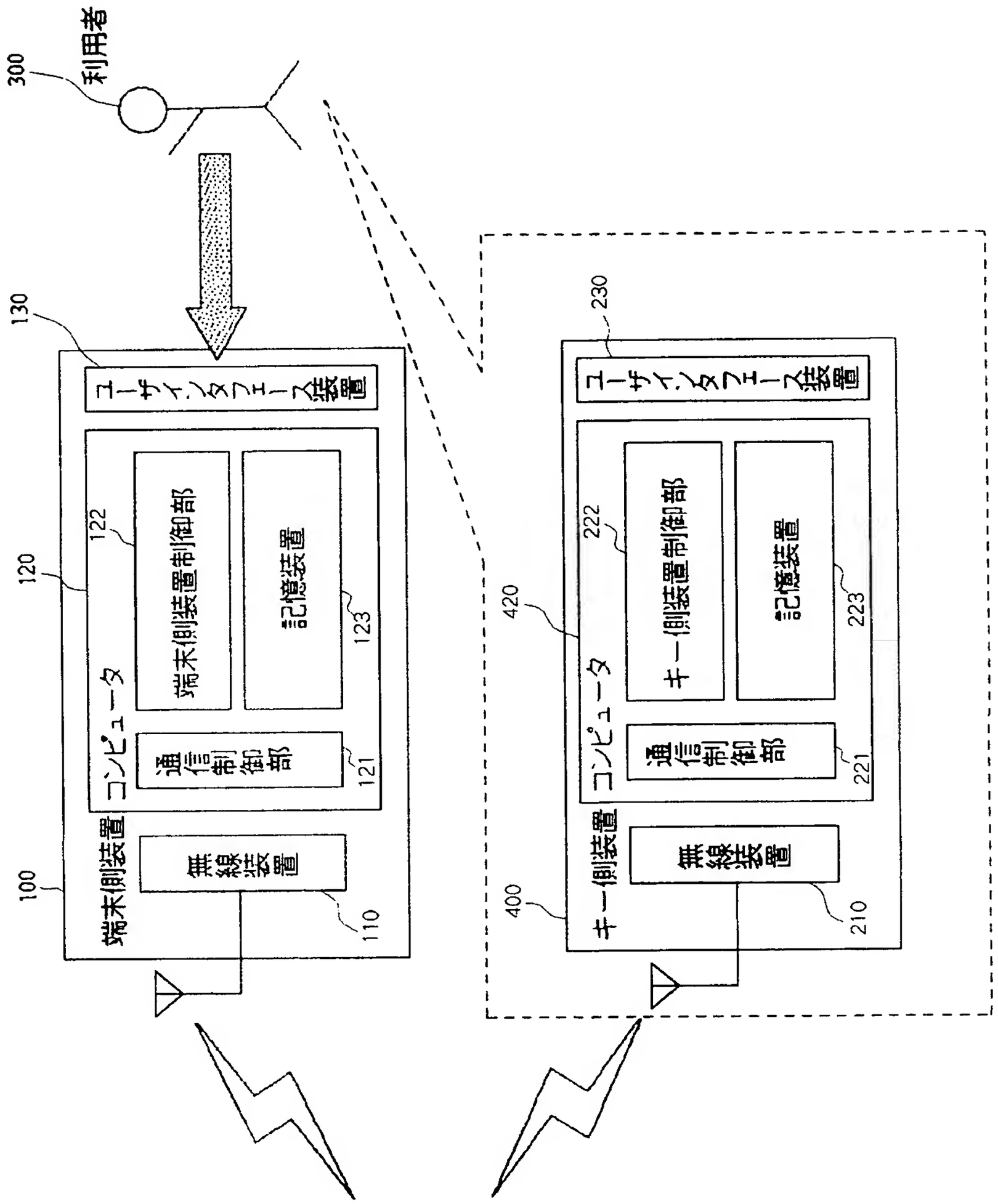


出証特２００３－３０５９６４７

【図３】


キー側装置スタート
端末側装置からの
接続の待ち受け
21
No
接続に成功？
22
Yes
23
端末側装置との
接続を維持
24
接続が切断された？
No
Yes

【図４】


300
利用者
130
ユーザインタフェース装置
120
コンピュータ
122
端末側装置制御部
記憶装置
123
通信制御部
121
端末側装置
無線装置
110
100
230
ユーザインタフェース装置
420
コンピュータ
222
キー側装置制御部
記憶装置
223
通信制御部
221
キー側装置
無線装置
210
400

【書類名】　要約書

【要約】

【課題】　利用者に煩雑な操作を要求することなく本人確認を行い、第三者による端末装置の不正使用を確実に防止する。

【解決手段】　端末側装置１００は保護したい端末装置に装着され、キー側装置２００は利用者が身につけて携帯する。端末側装置１００の記憶装置１２３には、キー側装置２００の情報が登録されている。キー側装置２００を身につけた利用者が端末側装置１００を装着した端末装置から離れ、端末側装置１００とキー側装置２００との間でブルートゥース、無線ＬＡＮ等の近距離無線通信による接続ができなくなると、端末側装置１００は装着されている端末装置の使用を禁止してロック状態とする。

【選択図】　図１

特願２００２－２６４０７２

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社